AF/IFW

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

PATENT APPLICATION

ATTORNEY DOCKET NO. 200205371-1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s):	Chris Hyser	Confirmation No.:	2604
Application No.:	10/693,182	Examiner:	Devin E. Almeida
Filing Date:	October 23, 2003	Group Art Unit:	2132

Title: METHOD AND SYSTEM FOR PROVIDING AN EXTERNAL TRUSTED AGENT FOR ONE OR MORE COMPUTER SYSTEMS

Mail Stop Appeal Brief-Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on February 10, 2008 .

The fee for filing this Appeal Brief is (37 CFR 1.17(c)) $500.00.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

□ (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d)) for the total number of months checked below:

□ 1st Month $120   □ 2nd Month $450   □ 3rd Month $1020   □ 4th Month $1590

□ The extension fee has already been filed in this application.

☒ (b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge to Deposit Account 08-2025 the sum of $ 500 . At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees.

☒ A duplicate copy of this transmittal letter is enclosed.

☒ I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, Alexandria, VA 22313-1450

Date of Deposit: May 12, 2008

OR

□ I hereby certify that this paper is being transmitted to the Patent and Trademark Office facsimile number (571)273-8300.

Date of facsimile:

Typed Name: Joanne Bourguignon

Signature: Joanne Bourguignon

Respectfully submitted,

Chris Hyser

By Robert W. Bergstrom

Robert W. Bergstrom

Attorney/Agent for Applicant(s)

Reg No. : 39,906

Date : May 12, 2008

Telephone : 206.621.1933

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re patent application of:

Applicant:	Chris Hyser
Application No.:	10/693,182
Filed:	October 23, 2003
Title:	METHOD AND SYSTEM FOR PROVIDING AN EXTERNAL TRUSTED AGENT FOR ONE OR MORE COMPUTER SYSTEMS

Examiner:	Devin E. Almeidal
Art Unit:	2132
Docket No.:	200205371-1
Date :	May 12, 2008

APPEAL BRIEF

Mail Stop: Appeal Briefs – Patents
Commissioner of Patents and Trademarks
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This appeal is from the decision of the Examiner, in an Office Action mailed December 10, 2007, finally rejecting claims 1-18.

REAL PARTY IN INTEREST

The real party in interest is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249 Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

RELATED APPEALS AND INTERFERENCES

Applicant's representative has not identified, and does not know of, any other appeals of interferences which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

STATUS OF CLAIMS

Claims 1-18 are pending in the application. Claims 1-18 were finally rejected in the Office Action dated December 10, 2007. Applicants' appeal the final rejection of claims 1-18 which are copied in the attached CLAIMS APPENDIX.

STATUS OF AMENDMENTS

No Amendment After Final is enclosed with this brief. The last Response was filed November 2, 2007.

SUMMARY OF CLAIMED SUBJECT MATTER

Independent Claim 1

Claim 1 is directed to a monitor (502 in Figure 5; Current Application, page 7, lines 3-13) that monitors the security state of a remote computer system, the monitor comprising: (1) a computing device; (2) a communications medium (506 in Figure 5; Current Application, page 7, lines 3-13) interconnecting the computing device with the remote computer system; (3) a pair of data-storage media each containing a sequence of encryption keys, one data-storage medium local to the monitor (510 in Figure 5; Current Application, page 7, lines 3-13), and the other data-storage medium (512 in Figure 5; Current Application, page 7, lines 3-13) local to the remote computer system; and (4) a program, running on the computing device, that exchanges with the remote computer system, over the communications medium, messages encrypted using one or more encryption keys extracted from the data-storage medium local to the remote computer system in order to monitor the security state of the remote computer system (Current Application, page 6, line 18 to page 7, line 2; Current Application, page 8, lines 25-29; and Current Application, page 9, line 14 to page 33, line 7).

Dependent Claims 2-8

Claim 2 is directed to the monitor (502 in Figure 5; Current Application, page 7, lines 3-13) of claim 1 wherein, following power on or reset of the remote computer system, while the remote computer system is in a relatively high-security state, the remote computer system sends an initial-authentication message (Current Application, page 14, lines 10-20; page 22, line 10 - page 25, line 28) to the monitor, encrypted with a next key extracted from the data-storage medium local to the remote computer system. Claim 3 is directed to the monitor (502 in Figure 5; Current Application, page 7, lines 3-13) of claim 2 wherein the monitor receives the initial-authentication message (Current Application, page 14, lines 10-20; page 22, line 10 - page 25, line 28), decrypts the initial-authentication message using a next key extracted from the data-storage medium local to the monitor, and stores an indication that the remote computer system is in a relatively high-security state. Claim 4 is directed to the monitor (502 in Figure 5; Current Application, page 7, lines 3-13) of claim 2 wherein the remote computer system collects security metrics and includes the security metrics in the initial-authentication message (Current Application, page 14, lines 10-20; page 22, line 10 - page 25, line 28). Claim 5 is directed to the monitor (502 in Figure 5; Current Application, page 7, lines 3-13) of claim 4 wherein the monitor receives the initial-authentication message (Current Application, page 14, lines 10-20; page 22, line 10 - page 25, line 28) and extracts the security metrics in order to determine the security state of the remote computer system. Claim 6 is directed to the monitor (502 in Figure 5; Current Application, page 7, lines 3-13) of claim 1 wherein, while the remote computer system is in a relatively high-security state, prior to loading and/or executing an untrusted software program into memory, the remote computer system sends a going-insecure message to the monitor (Current Application, page 25, line 29 - page 27, line 8), encrypted with a current key extracted from the data-storage medium local to the remote computer system. Claim 7 is directed to the monitor (502 in Figure 5; Current Application, page 7, lines 3-13) of claim 6 wherein the monitor receives the going-insecure message, decrypts the initial-authentication message using a current key extracted from the data-storage medium local to the monitor, and stores an indication that the remote computer system is in a relatively low-security state (Current Application, page 28, line 27 - page 33, line 7). Claim 8 is directed to the monitor (502 in Figure 5; Current Application, page 7, lines 3-13) of claim 1 wherein the data-storage media both contain identical sequences of encryption keys, and each of the data-storage media are one of: a compact disc; a DVD disc; an electronic memory; and a magnetic disk.

Independent Claim 9

Claim 9 is directed to a method for monitoring and reporting the security state of a remote computer system, the method comprising: (1) providing a monitor (502 in Figure 5; Current Application, page 7, lines 3-13) computing device interconnected with the remote computer system by a communications medium (506 in Figure 5; Current Application, page 7, lines 3-13); (2) providing a pair of data-storage media, each containing a sequence of encryption keys, one data-storage medium (510 in Figure 5; Current Application, page 7, lines 3-13) local to the monitor computing device, and the other data-storage medium (512 in Figure 5; Current Application, page 7, lines 3-13) local to the remote computer system; and (3) receiving messages from the remote computer system over the communications medium by the monitor and storing an indication, by the monitor, of the security state of the remote computer system determined by the monitor from the received messages (Current Application, page 6, line 18 to page 7, line 2; Current Application, page 8, lines 25-29; and Current Application, page 9, line 14 to page 33, line 7).

Dependent Claims 10-18

Claim 10 is directed to the method of claim 9 further including receiving, by the monitor (502 in Figure 5; Current Application, page 7, lines 3-13), a request for information about the security state of the remote computer system, and replying with a security-status-inquiry-response message by the monitor based on a determined security state of the remote computer system (Current Application, page 29, lines 20-45). Claim 11 is directed to the method of claim 9 further including, following power on or reset of the remote computer system, while the remote computer system is in a relatively high-security state, sending, by the remote computer system, an initial-authentication message (Current Application, page 14, lines 10-20; page 22, line 10 - page 25, line 28) to the monitor (502 in Figure 5; Current Application, page 7, lines 3-13), encrypted with a next key extracted from the data-storage medium local to the remote computer system. Claim 12 is directed to the method of claim 11 further including receiving, by the monitor (502 in Figure 5; Current Application, page 7, lines 3-13), the initial-authentication message (Current Application, page 14, lines 10-20; page 22, line 10 - page 25, line 28), decrypting the initial-authentication message using a next key extracted from the data-storage medium local to the monitor, and storing an indication that the remote computer system is in a relatively high-security state.

Claim 13 is directed to the method of claim 11 further including collecting, by the remote computer system, security metrics and including the security metrics in the initial-authentication message (Current Application, page 14, lines 10-20). Claim 14 is directed to the method of claim 13 further including receiving, by the monitor (502 in Figure 5; Current Application, page 7, lines 3-13), the initial-authentication message (Current Application, page 14, lines 10-20; page 22, line 10 - page 25, line 28) and extracting the security metrics in order to determine the security state of the remote computer system. Claim 15 is directed to the method of claim 9 further including sending, by the remote computer system, a going-insecure message to the monitor (Current Application, page 25, line 29 - page 27, line 8), encrypted with a current key extracted from the data-storage medium local to the remote computer system, while the remote computer system is in a relatively high-security state, prior to loading and/or executing an untrusted software program into memory. Claim 16 is directed to the method of claim 15 further including receiving, by the monitor (502 in Figure 5; Current Application, page 7, lines 3-13), the going-insecure message, decrypting the going-insecure message using a current key extracted from the data-storage medium local to the monitor, and storing an indication that the remote computer system is in a relatively low-security state (Current Application, page 28, line 27 - page 33, line 7). Claim 17 is directed to Computer instructions implementing the method of claim 9 encoded in a computer-readable medium. Claim 18 is directed to a monitor (502 in Figure 5; Current Application, page 7, lines 3-13) that monitors the security state of a computer system by the method of claim 9.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. The rejection of claims 1-18 under 35 U.S.C. §103(a) as being unpatentable over Schneck et al., U.S. Patent No. 6,865,426 in view of Jones, U.S. Patent No. 5,412,730.

ARGUMENT

Claims 1-18 are pending in the current application. In an office action dated December 10, 2007 ("Office Action"), the Examiner finally rejected claims 1-18 under 35 U.S.C. §103(a) as being unpatentable over Schneck et al., U.S. Patent No. 6,865,426 ("Schneck") in view of Jones, U.S. Patent No. 5,412,730 ("Jones"). Applicant's representative respectfully traverses these rejections.

ISSUE 1

1. The rejection of claims 1-18 under 35 U.S.C. §103(a) as being unpatentable over Schneck et al., U.S. Patent No. 6,865,426 in view of Jones, U.S. Patent No. 5,412,730.

While the recent U.S. Supreme Court decision, *KSR International Co. v. Teleflex Inc*,. rejected the overly rigid and formalistic application of the Federal Circuit's teaching-suggestion-motivation ("TSM") test, as discussed in M.P.E.P. §2141(I), the *KSR* decision provided useful direction with regard to obviousness-type rejections. First of all, as discussed in M.P.E.P. §2141(II), *KSR* again emphasized that obviousness is a question of law based on underlying factual inquiries, including ascertaining the differences between the claimed invention and the prior art and resolving the level of ordinary skill in the pertinent art, and reemphasized the *Graham* factors. M.P.E.P. §2141(II) emphasizes the fact that examiners, in making obviousness-type rejections, "fulfill the critical role of fact finder when resolving the *Graham* inquiries. It must be remembered that while the ultimate determination of obviousness is a legal conclusion, the underlying *Graham* inquiries are factual." Furthermore, in Applicant's representative's respectfully offered opinion, *KSR* clearly apportions significant responsibility and burdens on examiners, as discussed in M.P.E.P. §2141(III):

> The key to supporting any rejection under 35 U.S.C. 103 is the clear articulation of the reason(s) why the claimed invention would have been obvious. The Supreme Court in *KSR* noted that the analysis supporting a rejection under 35 U.S.C. 103 should be made explicit. The court quoting *In Re Kahn*, 441 F.3d 977, 988, 78 U.S.P.Q.2d 1329, 1336 (Fed.Cir. 2006), stated that "'[R]ejections on obviousness cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.'"

In Applicant's representative's respectfully offered opinion, the Examiner has erred both in legal conclusions as well as in basic fact finding, and has failed to offer a rational underpinning and rational argument to support the Examiner's obviousness-type rejection. Applicant's representative first addresses the improper legal conclusion made by the Examiner, and then addresses what Applicant's representative respectfully believes to be the Examiner's failure to understand the currently claimed invention, the cited prior art references, and the fundamental difference between them, as well as offering analysis directed to irrelevant arguments and conclusions.

In a response to a previous office action, filed by Applicant on November 2, 2007, Applicant's representative, on page 6, pointed out that "claim 1 is directed to the monitoring of the security state of one computer system by another, as is stated repeatedly in both the preambles and the final elements of independent claims 1 and 9." In the Office Action, the Examiner states:

> In response to applicant's arguments, the recitation "a monitor that monitors the security state of a remote computer system, the monitor comprising" has not been given patentable weight because the recitation occurs in the preamble. A preamble is generally not accorded any patentable weight where it merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand alone. See *In re Hirao*, 535 F.2d 67, 190 USPQ 15 (CCPA 1976) and *Kropa v. Robie*, 187 F.2d 150, 152, 88 USPQ 478, 481 (CCPA 1951).

Apparently the Examiner has overlooked the fact that the language "monitor the security state of the computer system" in the final element of claim 1, and the language "storing an indication, by the monitor, of the security state of the computer system determined by the monitor," of claim 9, both include language directed to a monitor that monitors the security state of a computer system directly within the body of two independent claims. The language "to monitor the security state of the computer system" in the final element of claim 1 refers to the language "monitor that monitors the security state of a remote computer system" in the preamble of claim 1. The language "the monitor, of the security state of the remote computer system determined by the monitor from the received messages" in the last element of claim 9 directly references the language "method for monitoring and reporting the security state of a remote computer system" in the preamble of claim 9. Note that, for example, the phrases "the remote computer system" in the first elements of claims 1 and 9 would lack antecedent basis were they not recognized as referring to the language "a remote computer system" in the preambles of claims 1 and 9. As those familiar with claim interpretation well understand, there is no rigid, fixed proscription against according patentable weight to language recited in the preamble of a claim. Note that, even in the statement made by the Examiner, a "preamble is generally not accorded any patentable weight . . . where the body of the claim does not depend on the preamble for completeness." Obviously, when claim terms depend on language recited in the preamble for antecedent basis, the body of a claim most definitely depends on the preamble for completeness. According to current case law, when the body of the claim "sets out the complete invention," the preamble is not ordinarily treated as limiting the scope of the claim. *Schumer v. Lab. Computer Sys., Inc.*, 308 F.3d 1304, 1310 (Fed. Cir. 2002). However, the preamble is regarded as limiting if it recites essential structure that is important to the invention or necessary to give meaning to the claim. *NTP, Inc. v. Research In Motion, Ltd.*, 418 F.3d 1282, 1305-06 (Fed. Cir. 2005), *cert. denied*, 74 U.S.L.W. 3421 (U.S. Jan. 23, 2006); *SanDisk Corp. v. Memorex Prods., Inc.*, 415 F.3d 1278, 1284 n.2 (Fed. Cir. 2005), *cert. denied*, 126 S. Ct. 829 (2005). That is, if the claim drafter "chooses to use both the preamble and the body to define the subject matter of the claimed invention, the invention so defined, and not some other, is the one the patent protects." *Bell Commc'ns Research, Inc. v. Vitalink Commc'ns Corp.*, 55 F.3d 615, 620 (Fed. Cir. 1995) (emphasis in original). **Moreover, when the limitations in the body of the claim "rely upon and derive antecedent basis from the preamble, then the preamble may act as a necessary component of the claimed invention."** *Eaton Corp. v. Rockwell Int'l Corp.*, 323 F.3d 1332, 1339 (Fed. Cir. 2003).

One large difference between the currently claimed invention and the teachings of both Schneck and Jones is that the currently claimed invention is directed to a remote computer-system monitor that monitors and reports the security state of a remote compute system. By contrast, both Jones and Schneck are directed to secure communications between computer systems. These are very different problems. In the current application, the monitored computer does not trust the computer that it monitors while, by contrast, in both Jones and Schneck's disclosed communications systems, both computers party to communications necessarily and inherently trust one another. Neither Jones nor Schneck is concerned with verifying whether or not one of the two computers party to communications can be trusted, but instead are directed to a communications system to prevent access to those communications by parties other than the two parties communicating. This is an entirely different type of security than the security to which the current application is directed. For example, Jones can employ pseudo-random-number generators, in both computer systems communicating by Jones' method, because the operating system and the communications support within the operating system of both computers is trusted to properly employ the pseudo-random-number generators for secure communications. However, were either of Jones' communicating computers unable to trust the computer with which it is communicating, then symmetrical pseudo-random-number generators on both computer systems would be insufficient to secure communications. The Examiner has failed to appreciate the difference between monitoring the security level of the computer system and securing communications between two computers that trust one another, and has attempted to avoid considering clear claim language directed to the difference by incorrectly asserting that the claim language occurs only in the preamble, and thus can be ignored. For this reason, alone, the Examiner's arguments entirely fail the standards of KSR and M.P.E.P. §2141.

On page 3 of the Office Action, the Examiner states that "Schneck teaches a monitor that monitors the security state of a remote computer system." Schneck does not teach a monitor that monitors the security state of a remote computer system. Applicant's representative addressed this point in a previously filed response to a previously issued office action. Applicant's representative includes a portion of the previously filed response to again address this point:

> Operation of Schneck's secure communications system is described in the following passages of Schneck, the first beginning on line 35 of column 4 and the second beginning on line 11 of column 6.
>
>> The send host 103 includes a signature generator 116 which generates a signature block 119 from the data block 109 and the key 113 using a predetermined security algorithm which may be, for example, but not limited to, a security algorithm such as the Digital Signature Algorithm (DSA), the Rivest-Sharnir-Adleman (RSA) algorithm, or secret key authentication, which are generally known in the art.
>>
>> The send host 103 also includes an authentication header generator 123, which generates an authentication header 126. The authentication header 126 includes various data fields, such as, for example, an authentication sequence number, data frame size, frame type, security algorithm, verification type, minimum security level, target security level, and an actual security level. T*he receive host 106 employs these data fields to generate an actual security configuration to achieve authentication of a data stream communicated from the send host 103.* The actual security configuration is dynamic in that it may be changed by either the send host 103 or the receive host 106 during the course of data communication therebetween in response to user or application requirements, or changes in computer resource availability as will be discussed. (emphasis added)
>>
>> *Generally, the security levels as discussed herein refer to the percentage of verified data packets in the receive host 106. The security monitor 169 also determines the verification type as indicated by the first functional switch 153, as well as the specific security algorithm employed by both the delayed authentication verifier 156 and the percentage authentication verifier 163.*
>>
>> T*he security monitor 169 attempts to specify an actual verification type, actual security algorithm, and an actual security level according to the desired security configuration received from the send host 103. However, the receive host 106 may not have enough*

> *processor time or security operations per second (SOPS) to provide the desired security configuration due to the verification of other data streams which currently employ much of not all of the SOPS available in the receive host 106 at a given moment. Consequently, the security monitor 169 may force a change in the verification type, security algorithm, and/or the actual security level that differs from the desired security configuration received by the send host 103 in order to accommodate the data stream.* (emphasis added)
>
> As the Examiner can hopefully appreciate, there is no teaching or suggestion that send host 103 monitors the security state of receive host 106. *Schneck is not concerned with, or directed to, the security state of any computer system.* Instead, Schneck is concerned with a negotiated, secure communication of data between two computer systems. The security levels discussed in Schneck "refer to the percentage of verified data packets in the receive host 106," as explicitly stated by Schneck. These security levels have nothing to do with the security state of either computer system (103 and 106), but instead to the degree to which communications between the two computer systems are secured by application of communications security techniques. It would seem that the Examiner noticed block 169, labeled "Security Monitor," in Figure 1 of Schneck and immediately assumed that this block was concerned with monitoring the security state of a computer system. As can be readily observed in the above-quoted passages, block 169 is concerned with configuring secure communications on the receive host according to information contained in data messages sent to the receive host by the send host. This box does not represent anything that monitors the security state of another computer.

The Examiner has not responded to Applicant's representative's argument in the Office Action, but simply restated the rejection, referring to various elements of Figure 1 and to Schneck's abstract. Schneck's abstract reads as follows:

> ***The present disclosure relates to a method for communicating and applying adaptive security to a data stream comprising a plurality of data packets.*** The method comprises the steps of identifying a desired security level range and a desired actual security level which falls within the desired security level range. The availability of a number of security processor operations at the host is determined so that, if needed, computing resources at the host can be reallocated to ensure that the data stream can be verified at the desired actual security level. If there are not sufficient resources available for reallocation at the host, communication resources can be reallocated, for example by changing the bandwidth of the data stream or another incoming data stream. With this method, the actual security level will be kept within the desired security level range. (emphasis added)

It is clear from this abstract that Schneck discloses a method for securing communications, and monitoring the resources available on a remote computer system in order to secure communications to a desired level. Schneck has absolutely nothing whatsoever to do with monitoring the security state of a remote computer system. In Applicant's representative's respectfully offered opinion, the Examiner has not only failed to appreciate the rather large differences between the security monitor disclosed in the current application and Schneck, but has completely failed to provide the rational underpinning for the conclusory statement that "Schneck teaches a monitor that monitors the security state of a remote computer system," without providing even rudimentary analysis or justification, other than referencing a few elements in Figure 1 of Schneck and Schneck's abstract. There is no discussion or analysis provided by the Examiner as to why the abstract is viewed by the Examiner as teaching a "monitor that monitors the security state of a remote computer system." The Examiner has clearly relied on incorrect fact finding in the Examiner's obviousness rejection, and the obviousness rejection, for this reason, clearly fails the fail the standards of KSR and M.P.E.P. §2141.

The Examiner further states, in rejecting claim 1:

> Schneck teach using encrypted communication between the devices but does not teach a pair of data-storage media each containing a sequence of encryption keys, one data-storage medium local to the monitor, and the other data-storage medium local to the remote computer system; and a program, running on the computing device, that exchanges with the remote computer system, over the communications medium, messages encrypted using one or more encryption keys extracted from the data-storage medium local to the remote computer system in order to monitor the security state of the remote computer system. Jones teaches a pair of data-storage media each containing a sequence of encryption keys (see Jones figure 1 element 23 and 27), one data-storage medium local to the monitor (see Jones figure 1 element 27), and the other data-storage medium local to the remote computer system (see Jones figure 1 element 23 and 27 and abstract).

Applicant's representative, like the previous point, addressed this point in the same, previously filed response to a previously issued office action:

> However, in the current Office Action, the Examiner has again relied on references that do not teach, mention, or suggest the second element of claim 1 "a pair of data-storage media each containing a sequence of encryption keys, one data-storage medium local to the monitor, and the other data-storage medium local to the remote computer system" and the second element of claim 9 "providing a pair of data-storage media, each containing a sequence of encryption keys, one data-storage medium local to the monitor computing device, and the other data-storage medium local to the remote computer system."
>
> One embodiment of the data-storage media to which the

> second elements of claims 1 and 9 are directed is shown in Figure 6 of the current application. In the described embodiment, the data-storage media are CD-read/write devices. The CD-read/write devices and are shown positioned within a system (510 and 512) in Figure 5 of the current application.
>
> The Examiner states, on page 3 of the Office Action, that "Jones teaches a pair of data-storage media each containing a sequence of encryption keys (see Jones figure 1 element 23 and 27)." Elements 23 and 27 of Figure 1 of Jones are pseudo-random number generators, and are clearly labeled as such. Those familiar with electronics and computing well understand that a pseudo-random number generator is not a sequence of encryption keys, but is instead an electronic circuit or executable routine that generates pseudo-random numbers by one of many possible pseudo-random-number-generation algorithms. These pseudo-random-number-generation algorithms generally employ a seed number or value to initialize the circuit or routine, and then generate pseudo-random numbers one after another, when requested to do so. Indeed, Jones describes operation of the pseudo-random number generator (23 in Figure 1), beginning on line 34 of column 3, as follows:
>
>> The advance signal produced by block counter 21 is supplied to the advance input of a pseudo-random number generator 23 which supplies a sequence of encryption key values to the key input of the encryptor 17. *The content of the key sequence is predetermined by the combination of (1) the internal makeup of the generator 23 and by (2) a supplied random number seed value which initializes the generator 23. The generator 23 responds to each advance signal from block counter 21 by changing its output to the next successive encryption key value.* (emphasis added)
>
> A pseudo-random number generator is not a data-storage medium containing a sequence of encryption keys. Jones does not teach, mention, suggest, or even imply any kind of pair of data-storage media, each containing a sequence of encryption keys. Indeed, Jones' pseudo-random number generator supply an electronically encoded sequence of pseudo-random numbers, but do so one pseudo-random number at a time, and generate each pseudo-random number algorithmically, rather than employing a stored list of pseudo-random numbers. That is why they are called "pseudo-random number <u>generators</u>," and not "sequences of pseudo-random numbers," as anyone familiar with computer science well understands.

In this case, the Examiner did attempt to respond to the previously supplied argument by stating: "Jones clearly teaches that both the transmitting station (computing device) and the receiving station (remote computer system) have a sequence of encryption keys that are changed at predetermined times (see Figure 1 and abstract)." However, the fact that the two parties to the communications system in Jones both employ pseudo-random-number generators does not, in any way, imply that Jones teaches, mentions, or discloses "a pair of data-storage media each containing a sequence of encryption keys, one data-storage medium local to the monitor, and the other data-storage medium local to the remote computer system." There is certainly nothing in Jones' abstract to suggest that either computer stores, on a data-storage medium, a sequence of encryption keys. As Applicant's representative previously stated, pseudo-random-number generators are well known to those familiar with computer science, and are generally hardware-implemented or software-implemented algorithmic routines for ***generating*** random numbers. In many cases, a pseudo-random-number-generator routine is initialized using a seed value, and then provides a next pseudo-random number upon each routine call. Examples include the *rand()* and *srand()* functions widely available in C and C++ libraries. The numbers are generated algorithmically, and not stored. Otherwise, there would be no need for a "seed value." Pseudo-random-number generators, operated synchronously, provide the foundation for many different types of security systems, especially communications-security systems. However, in the case that the data stored within a computer cannot be assumed to be secure, a stored sequence of encryption keys would provide no foundation for any type of security system. Thus, the difference between storing a sequence of encryption keys and generating a sequence of encryption keys is quite large and quite profound, from the standpoint of computer security. The Examiner has failed to provide any discussion or analysis of this issue, other than claiming that, because pseudo-random-number generators are shown in Figure 1, and mentioned in the abstract, that Jones "clearly teaches that both the transmitting station (computer device) and the receiving station (remote computer system) have a sequence of encryption key." Because pseudo-random-number generators do not, generally, store sequences of encryption keys, the reasoning on which the Examiner bases this attempted justification is completely flawed, and certainly does not supply a rational underpinning for the Examiner's assertion. The Examiner states:

> It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have a pseudo-random number generator at the transmitting and receiving stations to supply a like sequence of encryption keys to both the encryptor and decryptor, without these keys being transmitted in any form over the transmission facility. Therefore one would have been motivated to have a pseudo-random number generator at the transmitting and receiving stations to supply a like sequence of encryption keys to both the encryptor and decryptor (see column 1 lines 37-53).

Applicant's representative respectfully submits that this statement makes no sense. If the

Examiner is asserting that it would have been obvious at the time of the invention to employ synchronously operating pseudo-random number generators as a foundation for secure communications, Applicant's representative heartily agrees. But, Applicants do not claim or disclose using pseudo-random-number generators.

The currently claimed invention is summarized, in the first paragraph of the detailed description of the invention in the current application:

> The present invention is related to computer-system security. A large effort is currently underway in the computing industry to provide secure computer systems to facilitate electronic commerce, storage of confidential information in commercial and governmental institutions, secure communications, and for facilitating construction of highly available, tamper-proof computer systems. Figure 1 is a block diagram of a number of important components within a single-processor computer-hardware platform. The hardware platform 101 includes a processor 103, random-access memory 105, and non-volatile data storage, such as a hard disk drive 107. The processor stores and retrieves data from memory 105 via a high-speed system bus 109. The high-speed system bus is interconnected to one or more lower-speed peripheral busses 111 via a system controller 113. A non-volatile data-storage controller 115 is connected to the peripheral bus 111 as well as to an input/output ("I/O") bus 117 which is connected to the non-volatile data-storage device 107. Additional I/O controllers, such as I/O controller 119, may be connected to the one or more peripheral busses 111.

The current application describes, with reference to Figures 5 and 6, an embodiment of an SMC security-state monitoring system. Figure 5 is described as follows:

> Figure 5 illustrates the hardware components involved in SMC security-state monitoring in the described embodiment of the present invention. As shown in Figure 5, the SMC 502, implemented using an external PC or other computing system, is connected by a communications medium 506 and a communications-medium controller 508 with a computer system 504, the security state of which it monitors. The SMC includes at least one CD-read/write device 510 for producing pairs of CDs containing encryption-key sequences, and for reading the security keys needed to communicate with a computer system whose security state it is currently monitoring. A computer system 504 monitored by the SMC also includes a CD-ROM device 512, or other device, capable of reading encryption keys from an encryption-key containing CD.

Figure 6 describes the CD pair shown in Figure 6 as follows:

> Figure 6 illustrates the contents of a CD pair that is concurrently used by the SMC in a computer system monitored by the SMC, and internal information stored by the computer system and the SMC to facilitate the data exchange that allows that SMC to monitor the security state of the computer

> system. As shown in Figure 6, the SMC prepares two identical CDs 602 and 604, each containing a sequence of encryption keys, in the case that symmetric encryption is employed, as well as a numerical identifier 605 that identifies the CD pair. In the case that asymmetric encryption is employed, the CDs contain sequences of complementary private and public encryption keys. In Figure 6, each symmetric key or asymmetric key pair is represented by a letter, such as the letter "A" representing the first key or key pair 606 of the sequence stored on the CDs. In either case, the encryption key or encryption-key pair stored at a particular location within the sequence on a disc can be used by the computer system and the SMC to encrypt messages that are exchanged between the computer system and SMC that allow the SMC to monitor the security state of the computer system. In Figure 6, a first CD 602 is maintained in physical collocation with the SMC, and a second computer disc 604 is provided to the system administrator of the computer system. Within the computer system, the current index, or key tag, may be stored in memory 607, while in the SMC, a table of computer-system-identifiers/key-tag pairs is stored within a table 608. Each time a computer system is powered up or reset, the key tag is advanced in order to employ the next key or key pair in the sequence stored on the CD for communications with the SMC. Keys or key pairs are not reused.

With this background, claims 1 and 9 of the current application, provided below, can be seen to clearly claim the disclosed computer-security-state monitoring system disclosed in the current application:

> 1. A monitor that **monitors the security state of a remote computer system,** the monitor comprising:
>
> a computing device;
>
> a communications medium interconnecting the computing device with the remote computer system;
>
> a pair of data-storage media each containing a sequence of encryption keys, one data-storage medium local to the monitor, and the other data-storage medium local to the remote computer system; and
>
> a program, running on the computing device, that exchanges with the remote computer system, over the communications medium, messages encrypted using one or more encryption keys extracted from the data-storage medium local to the remote computer system **in order to monitor the security state of the remote computer system.** (emphasis added)
>
> 9. A method for **monitoring and reporting the security state of a remote computer system,** the method comprising:
>
> providing a monitor computing device interconnected with the remote computer system by a communications medium;
>
> providing a pair of data-storage media, each containing a sequence of encryption keys, one data-storage medium local to the monitor computing device, and the other data-storage medium local to the remote computer system; and
>
> receiving messages from the remote computer system over the

> communications medium by the **monitor and storing an indication, by the monitor, of the security state of the remote computer system determined by the monitor from the received messages.** (emphasis added)

The monitor (502 in Figure 5) is a separate, external computer system from the remote computer (504 in Figure 5). The monitor monitors the security state of the remote computer. Both the monitor and the computer system being monitored contain a data-storage medium containing a sequence of encryption keys (510 and 512 in Figure 5). The monitor employs a protocol comprising encrypted messages exchanged between the monitor and the computer system that is being monitored in order to monitor the security state of the remote computer system. In the above-quoted passage, it is clear that the SMC monitors the remote computer system to determine whether or not the remote computer system is secure, in the case that no untrusted programs have yet been run by the remote computer system, or insecure, as reported by secure processes on the remote computer system to the SMC prior to execution of an untrusted program.

The Examiner has failed to produce any analysis or discussion that could, in Applicant's representative's respectfully offered opinion, possibly be considered as a rational underpinning for asserting that either Schneck or Jones discloses anything at all related to monitoring of the security state of a remote computer system. Instead, the Examiner points to Schneck's abstract, without any further discussion or analysis, and has failed to respond to Applicant's representative's previous arguments. Schneck's abstract, quoted above, mentions nothing about monitoring the security state of a remote computer system. In Applicant's representative's respectfully offered opinion, claims 1 and 9 clearly state, both in the preambles and in the claim bodies, that the system in one case, and the method in the other case, are directed to monitoring the security state of a remote computer system. The rejection of claims 1 and 9 do not appear capable of satisfying the basic requirements for an obviousness-type rejection discussed in M.P.E.P. §2141(III). As mentioned above, and as clearly stated in the previously filed response to a previously issued office action, neither Jones nor Schneck has anything at all to do with monitoring the security state of a remote computer system. Instead, both are directed to securing communications between computer systems. Neither Schneck nor Jones teaches, discloses, or mentions maintaining a sequence of encryption keys on a data-storage medium in a remote computer being monitored, and in the monitor monitoring the remote computer. Neither Schneck nor Jones is related to the current disclosure.

Because independent claims 1 and 9 are clearly not shown to be obvious in view of Schneck or Jones, none of the dependent claims that depend from them have been shown to be obvious by the Examiner. In addition, the rejections of the dependent claims are as baseless as those of the independent claims. For example, in rejecting claim 2, the Examiner cites, for the following language:

> wherein, following power on or reset of the remote computer system, while the remote computer system is in a relatively high-security state, the remote computer system sends an initial-authentication message to the monitor, encrypted with a next key extracted from the data-storage medium local to the remote computer system

column 4, line 66 to column 5, line 24; column 7, line 55 to column 9, line 12; and lines 26-27 of column 10 of Schneck. The cited portions of Schenck do not mention or suggest anything related to the security state of a computer system. These passages do discuss a security configuration, but that is a set of user configuration parameters displayed on an output display device. A security level is mentioned, but, as quoted above from Schneck, beginning on line 11 of column 6: "Generally, the security levels as discussed herein refer to the percentage of verified data packets in the receive host 106" This has nothing to do with the security state of a computer system, but - instead, a level of security desired for a communications exchange. The passages discuss data blocks with authentication headers, but do not once mention or suggest "an initial-authentication message," an example of which can be found on lines 22-30 of page 14 of the Current Application. Of course, nothing in the passages teaches, mentions, or suggests "a next key extracted from the data-storage medium local to the remote computer system," as pointed out by the Examiner in the above-quoted passage, and again repeated as follows: "Schneck teach using encrypted communication between the devices but does not teach a pair of data-storage media each containing a sequence of encryption keys, one data-storage medium local to the monitor, and the other data-storage medium local to the remote computer system; and a program." The rejection is accompanied by no analysis, and no rational underpinning. It is factually incorrect. Furthermore, citing entire pages of a reference, without pointing to particular passages or teachings, would seem to fall far short of the *KSR* standards. The Examiner recites the same, unrelated passages over and over again, in the rejections of claims 3-7 and 13-16. Secure digital communications using data packets with authentication headers is certainly an interesting topic, but has nothing to with monitoring the security state of a remote computer system, other than the fact that, as with many other distributed processes or tasks, secure communications is employed for communicating data between the monitor and remote computer system.

CONCLUSION

In Applicant's representative's respectfully offered opinion, neither Schneck nor Jones teaches, mentions or suggests anything at all related to monitoring of the security state of one computer by another. Because both independent claims 1 and 9 are clearly and ambiguously directed to the monitoring of the security state of one computer system by another, neither Schneck nor Jones, alone or in combination, can possible make obvious the invention claimed in claims 1 and 9, or in any claim depending from claims 1 and 9.

Applicant respectfully submits that all statutory requirements are met and that the present application is allowable over all the references of record. Therefore, Applicant respectfully requests that the present application be passed to issue.

Respectfully submitted,
Philip J. Kuekes et al.
OLYMPIC PATENT WORKS PLLC

By Robert W. Bergstrom
Robert W. Bergstrom
Registration No. 39,906

Olympic Patent Works PLLC
P.O. Box 4277
Seattle, WA 98104
206.621.1933 telephone
206.621.5302 fax

CLAIMS APPENDIX

1. A monitor that monitors the security state of a remote computer system, the monitor comprising:

a computing device;

a communications medium interconnecting the computing device with the remote computer system;

a pair of data-storage media each containing a sequence of encryption keys, one data-storage medium local to the monitor, and the other data-storage medium local to the remote computer system; and

a program, running on the computing device, that exchanges with the remote computer system, over the communications medium, messages encrypted using one or more encryption keys extracted from the data-storage medium local to the remote computer system in order to monitor the security state of the remote computer system.

2. The monitor of claim 1 wherein, following power on or reset of the remote computer system, while the remote computer system is in a relatively high-security state, the remote computer system sends an initial-authentication message to the monitor, encrypted with a next key extracted from the data-storage medium local to the remote computer system.

3. The monitor of claim 2 wherein the monitor receives the initial-authentication message, decrypts the initial-authentication message using a next key extracted from the data-storage medium local to the monitor, and stores an indication that the remote computer system is in a relatively high-security state.

4. The monitor of claim 2 wherein the remote computer system collects security metrics and includes the security metrics in the initial-authentication message.

5. The monitor of claim 4 wherein the monitor receives the initial-authentication message and extracts the security metrics in order to determine the security state of the remote computer system.

6. The monitor of claim 1 wherein, while the remote computer system is in a relatively high-security state, prior to loading and/or executing an untrusted software program into memory, the remote computer system sends a going-insecure message to the monitor, encrypted with a current key extracted from the data-storage medium local to the remote computer system.

7. The monitor of claim 6 wherein the monitor receives the going-insecure message, decrypts the initial-authentication message using a current key extracted from the data-storage medium local to the monitor, and stores an indication that the remote computer system is in a relatively low-security state.

8. The monitor of claim 1 wherein the data-storage media both contain identical sequences of encryption keys, and each of the data-storage media are one of:

a compact disc;
a DVD disc;
an electronic memory; and
a magnetic disk.

9. A method for monitoring and reporting the security state of a remote computer system, the method comprising:

providing a monitor computing device interconnected with the remote computer system by a communications medium;

providing a pair of data-storage media, each containing a sequence of encryption keys, one data-storage medium local to the monitor computing device, and the other data-storage medium local to the remote computer system; and

receiving messages from the remote computer system over the communications medium by the monitor and storing an indication, by the monitor, of the security state of the remote computer system determined by the monitor from the received messages.

10. The method of claim 9 further including receiving, by the monitor, a request for information about the security state of the remote computer system, and replying with a security-status-inquiry-response message by the monitor based on a determined

security state of the remote computer system.

11. The method of claim 9 further including, following power on or reset of the remote computer system, while the remote computer system is in a relatively high-security state, sending, by the remote computer system, an initial-authentication message to the monitor, encrypted with a next key extracted from the data-storage medium local to the remote computer system.

12. The method of claim 11 further including receiving, by the monitor, the initial-authentication message, decrypting the initial-authentication message using a next key extracted from the data-storage medium local to the monitor, and storing an indication that the remote computer system is in a relatively high-security state.

13. The method of claim 11 further including collecting, by the remote computer system, security metrics and including the security metrics in the initial-authentication message.

14. The method of claim 13 further including receiving, by the monitor, the initial-authentication message and extracting the security metrics in order to determine the security state of the remote computer system.

15. The method of claim 9 further including sending, by the remote computer system, a going-insecure message to the monitor, encrypted with a current key extracted from the data-storage medium local to the remote computer system, while the remote computer system is in a relatively high-security state, prior to loading and/or executing an untrusted software program into memory.

16. The method of claim 15 further including receiving, by the monitor, the going-insecure message, decrypting the going-insecure message using a current key extracted from the data-storage medium local to the monitor, and storing an indication that the remote computer system is in a relatively low-security state.

17. Computer instructions implementing the method of claim 9 encoded in a computer-readable medium.

18. A monitor that monitors the security state of a computer system by the method of claim 9.

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

None.